1. (Currently Amended) A method for controlling access to a private computer system comprising:

operatively connecting an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system;

classifying applications running on ~~an~~ said untrusted computer system as running in one of a trusted application execution context and an untrusted application execution context; and

preventing said untrusted computer system from initiating a connection with ~~a trusted~~ said private computer system unless said untrusted computer system is running said application in said trusted application execution context,

wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system.

2. (Currently Amended) The method in claim 1, wherein said ~~trusted~~ private computer system can initiate connections with any execution context on said untrusted private computer system.

3. (Original) The method in claim 1, wherein only said untrusted application execution contexts of said applications on said untrusted system can initiate connections with said external computer system.

4. (Original) The method in claim 1, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names.

5. (Original) The method in claim 4, wherein said untrusted system assigns said distinctive application execution context names.

6. (Original) The method in claim 4, wherein said applications cannot change a name of an execution context in which said applications are running.

7. (Original) The method in claim 1, wherein connections originating on said external system can terminate only at said untrusted system and can only operate in said untrusted execution contexts.

8. (Currently Amended) The method in claim 1, wherein said untrusted application execution contexts are fenced off from said ~~trusted~~ private computer system such that said untrusted application execution application contexts cannot interrogate critical system data of said ~~trusted~~ private computer system.

9. (Currently Amended) A method for controlling access to a ~~trusted~~ private computer system comprising:

operatively connecting an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system;

determining a source initiating an execution context of an application running on ~~an~~ said untrusted system;

naming said execution context as a trusted application execution context or an untrusted application execution context based on said source; and

preventing said untrusted computer system from initiating a connection with said ~~trusted~~ private computer system unless said untrusted computer system is running said application in said trusted application execution context,

wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system.

10. (Currently Amended) The method in claim 9, wherein said ~~trusted~~ private computer system can initiate connections with any execution context on said untrusted computer system.

11. (Original) The method in claim 9, wherein only said untrusted application execution contexts of said applications on said untrusted system can initiate connections with an external computer system.

12. (Original) The method in claim 9, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names.

13. (Original) The method in claim 12, wherein said untrusted system assigns said distinctive application execution context names based on said source.

14. (Original) The method in claim 12, wherein said applications cannot change a name of an execution context in which said applications are running.

15. (Original) The method in claim 9, wherein connections originating on an external system can terminate only at said untrusted system and can only operate in said untrusted execution contexts.

16. (Currently Amended) The method in claim 9, wherein said untrusted application execution contexts are fenced off from said ~~trusted~~ private computer system such that said untrusted application execution application contexts cannot interrogate critical system data of said ~~trusted~~ private computer system.

17. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform a method for controlling access to a private computer system, said method comprising:

operatively connecting an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system;

classifying applications running on an untrusted computer system as running in one of a trusted application execution context and an untrusted application execution context; and

preventing said untrusted computer system from initiating a connection with a ~~trusted~~ said private computer system unless said untrusted computer system is running said application in said trusted application execution context,

wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system.

18. (Currently Amended) The program storage device in claim 17, wherein said ~~trusted~~ private computer system can initiate connections with any execution context on said untrusted computer system.

19. (Original) The program storage device in claim 17, wherein only said untrusted application execution contexts of said applications on said untrusted system can initiate connections with said external computer system.

20. (Original) The program storage device in claim 17, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names.

21. (Original) The program storage device in claim 20, wherein said untrusted system assigns said distinctive application execution context names.

22. (Original) The program storage device in claim 20, wherein said applications cannot change a name of an execution context in which said applications are running.

23. (Original) The program storage device in claim 17, wherein connections originating on said external system can terminate only at said untrusted system and can only operate in said untrusted execution contexts.

24. (Original) The program storage device in claim 17, wherein said untrusted application execution contexts are fenced off from said ~~trusted~~ private computer system such that said untrusted application execution application contexts cannot interrogate critical system data of said ~~trusted~~ private computer system.

25. (Currently Amended) A system for controlling access to a network comprising:

a ~~trusted~~ private computer system;

an untrusted computer system connected ~~to~~ between said ~~trusted~~ private computer system and ~~to~~ an external computer system, such that said external computer is prevented from communicating directly with said private computer system;

wherein said untrusted system includes applications classified as having trusted application execution contexts and untrusted application execution contexts, ~~and~~

wherein only said trusted application execution contexts of said applications on said untrusted system can initiate connections with said ~~trusted~~ private computer system, and

wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system.

26. (Currently Amended) The system in claim 25, wherein said ~~trusted~~ private computer system can initiate connections with any execution context on said untrusted computer system.

27. (Original) The system in claim 25, wherein only said untrusted application execution contexts of said applications on said untrusted system can initiate connections with said external computer system.

28. (Original) The system in claim 25, wherein said applications are classified as having said trusted application execution contexts and said untrusted application execution contexts based on distinctive application execution context names.

29. (Original) The system in claim 28, wherein said untrusted system assigns said distinctive application execution context names.

30. (Original) The system in claim 28, wherein said applications cannot change a name of an execution context in which said applications are running.

31. (Original) The system in claim 25, wherein connections originating on said external system can terminate only at said untrusted system and can only operate in said untrusted execution contexts.

32. (Currently Amended) The system in claim 25, wherein said untrusted application execution contexts are fenced off from said ~~trusted~~ private computer system such that said untrusted application execution application contexts cannot interrogate critical system data of said ~~trusted~~ private computer system.